Unit 1

Objective:

a) *To know about network security.*

b) *To know need of Network Security.*
c) To know about security principals.
d) To know about attacks and their types.
e) To know about cyber ethics.
f) To know about cyber law.

1.1 NETWORK SECURIY

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

A good security professional should possess two important skills:

(1) The sense of security

(2) The knowledge of security principles

1.2 Need of Network Security

The information security is needed for the following given reasons.

1. *To protect the secret information users on the net only. No other person should see or access it.*
2. *To protect the information from unwanted editing, accidently or intentionally by unauthorized users.*
3. *To protect the information from loss and make it to be delivered to its destination properly.*
4. *To manage for acknowledgement of message received by any node in order to protect from denial by sender in specific situations.*

5. *To restrict a user to send some message to another user with name of a third one.*

1.3 Principal of Security

Information security follows three overarching principles:

- *Confidentiality*

This means that information is only being seen or used by people who are authorized to access it.

- *Integrity*

This means that any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.

- *Availability*

This means that the information is accessible when authorized users need it.

1.4 Type of attacks

Browser attacks

Browser based attacks are the most common network attack shown in the data. They try to trick internet surfers into downloading malware that is disguised as a software application or an update.

- ***Brute force attacks***

Pay attention to your passwords. When a hacker tries to decode a password or pin number through trial and error. Various consecutive guesses are generated by automated software try to crack the password code. It is a type of network attack that is time consuming, and success is a result of computing power and weak passwords.

- *Denial of Service(DoS)*

When an attacker takes control of computers and uses them to flood a particular email with messages, or a website with enormous blocks of data.

- ***SSL attacks***

Secure Sockets Layer (SSL) establishes an encrypted link between a website and a browser, or a mail server and a mail client. It is a standard security technology that enables secure information to be safely delivered. A website secured by SSL begins with https. An SSL attack type intercepts the encrypted data before it can be encrypted, giving the attacker access to sensitive data including credit card information and social security numbers.

- ***Scans***

Scans are hostile searches on the internet for open ports through which attackers can gain access to a computer. Rather than one of the true types of network attacks, they are typically reconnaissance and seen as potential precursors to attack.

- ***Backdoor attacks***

Backdoors are applications that allow computers to be accessed remotely. Many backdoors are designed to bypass intrusion detection systems. Several attack strategies, including port binding, connect-back, and connect availability use can be employed through backdoors. Both hardware and software components can allow hackers access through malicious backdoors.

- ***DNS attacks***

Domain name servers (DNS) maintain a directory of domain names, and translate them into IP addresses.DNS spoofing is when data is introduced into the domain name system cache, causing the name server to return an incorrect IP address, which redirects traffic to an alternate computer selected by the attacker. DNS queries come through Port 53, which traditional firewalls leave open.

1.5 Cybercrime

Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using phones via SMS and online chatting applications.

1.6 Information Technology Act, 2000

The Government of India enacted the Information Technology (I.T.) Act with some major objectives to deliver and facilitate lawful electronic, digital, and online transactions, and mitigate cyber-crimes.

Salient Features of IT Act

The salient features of the I.T Act are as follows −

- *Digital signature has been replaced with electronic signature to make it a more technology neutral act.*
- *It elaborates on offenses, penalties, and breaches.*
- *It outlines the Justice Dispensation Systems for cyber-crimes.*
- *It defines in a new section that cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.*
- *It provides for the constitution of the Cyber Regulations Advisory Committee.*
- *It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.*

- *It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.*

Scheme ofI.TAct

The following points define the scheme of the I.T. Act −

- *The I.T. Act contains 13 chapters and 90 sections.*
- *The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.*
- *It commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition.*
- *Chapter 2 deals with the authentication of electronic records, digital signatures, electronic signatures, etc.*
- *Chapter 11 deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act.*
- *Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.*
- *The Act is embedded with two schedules. The First Schedule deals with Documents or Transactions to which the Act shall not apply. The Second Schedule deals with electronic signature or electronic authentication technique and procedure. The Third and Fourth Schedule are omitted.*

Application oft heI.TAct

As per the sub clause (4) of Section 1, nothing in this Act shall apply to documents or transactions specified in First Schedule. Following are the documents or transactions to which the Act shall not apply −

- *Negotiable Instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;*
- *A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;*
- *A trust as defined in section 3 of the Indian Trusts Act, 1882;*
- *A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;*
- *Any contract for the sale or conveyance of immovable property or any interest in such property;*
- *Any such class of documents or transactions as may be notified by the Central Government.*

Amendments Brought in the I.T Act

The I.T. Act has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.

- *The first schedule contains the amendments in the Penal Code. It has widened the scope of the term "document" to bring within its ambit electronic documents.*
- *The second schedule deals with amendments to the India Evidence Act. It pertains to the inclusion of electronic document in the definition of evidence.*
- *The third schedule amends the Banker's Books Evidence Act. This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression "Certified-copy" to include such printouts within its purview.*

- *The fourth schedule amends the Reserve Bank of India Act. It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.*

Intermediary Liability

Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts, stores or transmits that record or provides any service with respect to that record.

According to the above mentioned definition, it includes the following −

- *Telecom service providers*
- *Network service providers*
- *Internet service providers*
- *Web-hosting service providers*
- *Search engines*
- *Online payment sites*
- *Online auction sites*
- *Online market places and cyber cafes*

Highlights of the Amended Act

The newly amended act came with following highlights −

- *It stresses on privacy issues and highlights information security.*
- *It elaborates Digital Signature.*
- *It clarifies rational security practices for corporate.*

- *It focuses on the role of Intermediaries.*
- *New faces of Cyber Crime were added.*

1.7 IT Amendment Act (ITA-2008)

The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team.

The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; making the owner of a given IP address responsible for content accessed or distributed through it; and making corporations responsible for implementing effective data security practices and liable for breaches.

The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals. Section 69, for example, authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion.

1.8 Hacker

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security. Hackers are classified

according to the intent of their actions.

8.1 Types of Hackers

The following list classifies hackers according to their intent.

Ethical Hacker :

A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration testing and vulnerability assessments.

Cracker (Black hat):

A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

Grey hat:

A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner

Script kiddies:

A non-skilled person who gains access to computer systems using already made tools.

Hacktivist :

A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

1.9 Phreaker:

A hacker who identifies and exploits weaknesses in telephones instead of computers.

Unit 2

Objective:

a) *To know about cryptography.*

b) To know about IPSec, HTTP, Digital Signature

2.1 SECURING DATA OVER INTERNET

In order to provide useful services or to allow people to perform tasks more conveniently, computer systems are attached to networks and get interconnected. Unfortunately, the extended access possibilities also entail increased security risks as it opens additional avenues for an attacker.

In the case of an automation system which is remotely connected to the Internet, the information flow is from/to a control application that manages sensors and actuators via communication lines of the public Internet and the network of the automation system target it are explained below :

a) *Interruption:*

An asset of the system gets destroyed or becomes unavailable. This attack targets the source or the communication channel and prevents information from reaching its intended Attacks in this category attempt to perform a kind of denial-of-service (DOS).

b) *Interception:*

An unauthorized party gets access to the information by eavesdropping into the communication channel (e.g. wiretapping).

c) *Modification:*

The information is not only intercepted, but modified by an unauthorized party while in transit from the source to the destination. By tampering with the information, it is actively altered (e.g. modifying message content).

d) *Fabrication:*

An attacker inserts counterfeit objects into the system without having the sender doing anything. When a previously intercepted object is inserted, this processes is called replaying. When the attacker pretends to be the legitimate source and inserts his desired information, the attack is called masquerading (e.g. replay an authentication message, add records to a file).

The four classes of attacks listed above violate different security properties of the computer system.

1. *Desired security features*

A security property describes a desired feature of a system with regards to a certain type of attack. A common classification is listed below:

- ***Confidentiality:*** *This property covers the protection of transmitted data against its release to non-authorized parties. In addition to the protection of the content itself, the information flow should also be resistant against traffic analysis. Traffic analysis is used to gather other information than the transmitted values themselves from the data flow*
- ***Authentication:*** *Authentication is concerned with making sure that the information is authentic. A system implementing the authentication property assures the recipient that the data is from the source that it claims to be. The system must make sure that no third party can masquerade successfully as another source.*

• ***Non-repudiation:*** *This property describes the feature that prevents either sender or receiver from denying a transmitted message. When a message has been transferred, the sender can prove that it has been received. Similarly, the receiver*

can prove that the message has actually been sent.

- ***Availability:*** *Availability characterizes a system whose resources are always ready to be used. Whenever information needs to be transmitted, the*

communication channel is available and the receiver can cope with the incoming data. This property makes sure that attacks cannot prevent resources from being used for their intended purpose.

• ***Integrity****: Integrity protects transmitted information against modifications. This property assures that a single message reaches the receiver as it has left the sender, but integrity also extends to a stream of messages. It means that no messages are lost, duplicated or reordered and it makes sure that messages cannot be replayed. As destruction is also covered under this property, all data must arrive at the receiver. Integrity is not only important as a security property, but also as a property for network protocols. Message integrity must also be ensured in case of random faults, not only in case of malicious modifications.*

2.2 Cryptography

Cryptography is the science of secret writing is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

There are five primary functions of cryptography today:

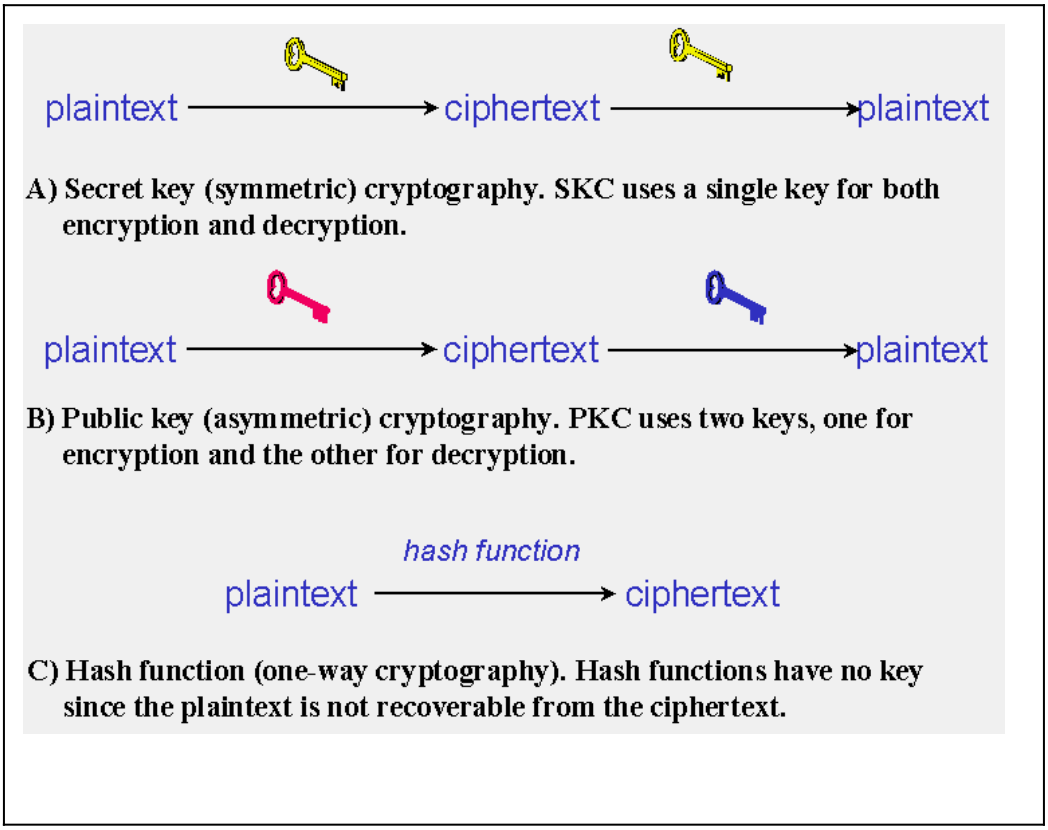
1. *Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.*
2. *Authentication: The process of proving one's identity.*
3. *Integrity: Assuring the receiver that the received message has not been altered in any way from the original.*
4. *Non-repudiation: A mechanism to prove that the sender really sent this message.*
5. *Key exchange: The method by which crypto keys are shared between sender and receiver.*

- *Cryptography Algorithms*

The three types of cryptography algorithms that will be discussed:

- *Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption; also called symmetric encryption. Primarily used for privacy and confidentiality.*
- *Public Key Cryptography (PKC): Uses one key for encryption and another for decryption; also called asymmetric encryption. Primarily used for authentication, non-repudiation, and key exchange.*
- *Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for*

message integrity.

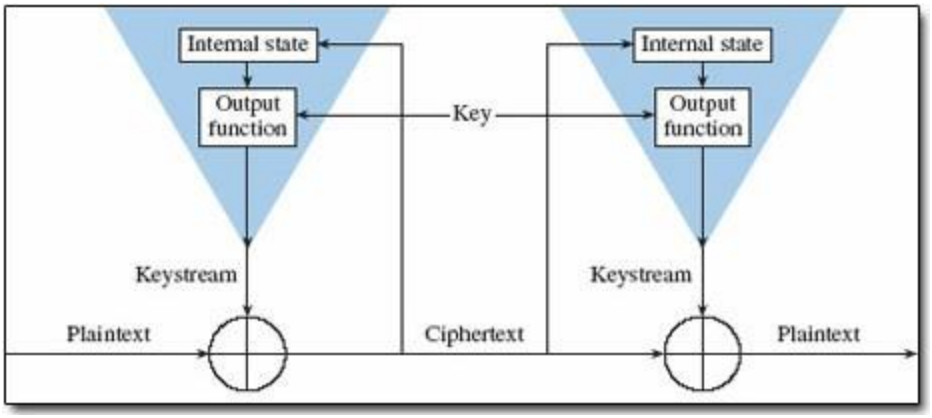


2.3 Secret Key Cryptography

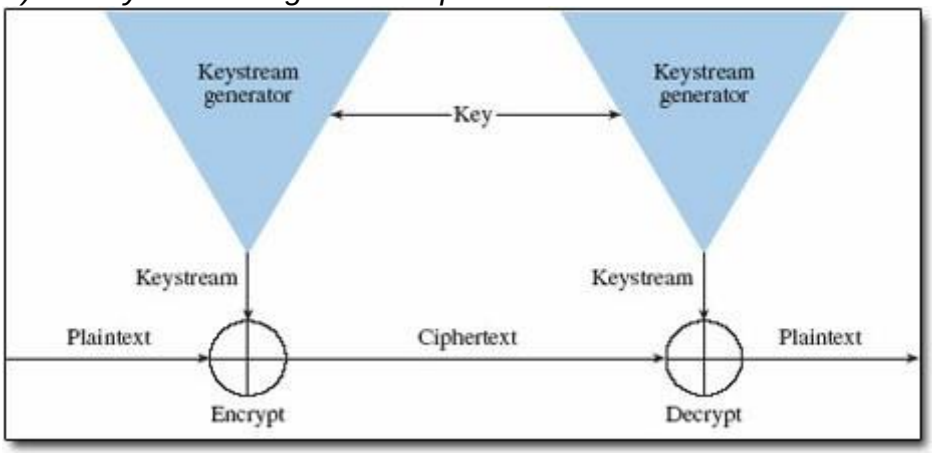
Secret key cryptography methods employ a single key for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key (more on that later in the discussion of public key cryptography).

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers.



A) Self-synchronizing stream cipher.



B) Synchronous stream cipher

- ***Secret key cryptography algorithms***

Data Encryption Standard(DES
Advanced Encryption Standard(AES):

Public Key Cryptography

PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to compute whereas their inverse function is relatively difficult to compute.

Generic PKC employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the cipher text. The important point here is that it does not matter which key is applied first, but that both keys are required for the process to work . Because a pair of keys are required, this approach is also called asymmetric cryptography.

In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme. Suppose Alice wants to send Bob a message. Alice encrypts some information using Bob's public key; Bob decrypts the ciphertext using his private key. This method could be also used to prove who sent a message; Alice, for example, could encrypt some plaintext with her private key; when Bob decrypts using Alice's public key, he knows that Alice sent the message (authentication) and Alice cannot deny having sent the message (non-repudiation).

Public key cryptography algorithms that are in use today for key exchange or digital signatures include:

2.4 RSA

- *RSA: The first, and still most common, PKC implementation, named for the three MIT mathematicians who developed it — Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length.*
- *Diffie and Hellman : After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm. D-H is used for secret-key key exchange only, and not for authentication or digital signatures.*
- *Elliptic Curve Cryptography (ECC): A PKC algorithm based upon elliptic curves. ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited compute power and/or memory, such as smartcards and PDAs.*

Public key cryptography: A set of interoperable standards and guidelines for public key cryptography, designed by RSA Data Security Inc.

  - *PKCS #1: RSA Cryptography Standard*
  - *PKCS #2: Incorporated into PKCS #1.*
  - *PKCS #3 and PKCS #4: Incorporated into PKCS #1.PKCS #5Password-Based Cryptography Standard*

Encryption *– Process of converting electronic data into another form, called cipher text, which cannot be easily understood by anyone except the authorized parties.This assures data security.*

Decryption*– Process of translating code to data.*

- *Message is encrypted at the sender's side using various encryption algorithms and decrypted at the receiver's end with the help of the decryption algorithms.*

- *When some message is to be kept secure like username, password, etc., encryption and decryption techniques are used to assure data security.*

2.5 Symmetric and Asymmetric cryptography

Types of Encryption

1. ***Symmetric Encryption***– *Data is encrypted using a key and the decryption is also done using the same key.*
2. ***Asymmetric Encryption****-Asymmetric Cryptography is also known as public key cryptography. It uses public and private keys to encrypt and decrypt data. One key in the pair which can be shared with everyone is called the public key. The other key in the pair which is kept secret and is only known by the owner is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.*

Public key– *Key which is known to everyone. Ex-public key of A is 7, this information is known to everyone.*
Private key– *Key which is only known to the person who's private key it is.*

Authentication*-Authentication is any process by which a system verifies the identity of a user who wishes to access it.*
Non- repudiation– *Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.*
Integrity– *to ensure that the message was not altered during the transmission.*

Message digest *-The representation of text in the form of a single string of digits, created using a formula called a one way hash function. Encrypting a message digest with a private key creates a digital signature which is an electronic means of authentication*

Secret Key Cryptography
This is the kind of cryptography that has been used for the transmission of secret information for centuries, long before the advent of computers. These algorithms require that the sender and the receiver agree on a key before communication is started.
Public Key Cryptography
Since the advent of public key cryptography, the knowledge of the key that is used to encrypt a plain text also allowed the inverse process, the decryption of the cipher text. In 1976, this paradigm of cryptography was changed by Diffie and Hellman [7] when they described their public key approach.
Authentication and Digital Signatures
An interesting and important feature of public key cryptography is its possible use for authentication. In addition to making the information unusable for attackers, a sender may utilize cryptography to prove his identity to the receiver. This feature is realized by digital signatures. A digital signature must have similar properties as a normal handwritten signature. It must be hard to forge and it has to be bound to a certain document.
Attack and Intrusion Detection
Attack detection assumes that an attacker can obtain access to his desired targets and is successful in violating a given security policy. Mechanisms in this

class are based on the optimistic assumption that most of the time the

information is transferred without interference. When undesired actions occur, attack detection has the task of reporting that something went wrong and then to react in an appropriate way. In addition, it is often desirable to identify the exact type of attack. An important facet of attack detection is recovery.

2.6 Pretty Good Privacy (PGP)

With the explosively growing reliance on electronic mail for every conceivable purpose, there grows a demand for authentication and confidentiality services. Two schemes stand out as approaches that enjoy widespread use: Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension (S/MIME). The latter is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security. Although both PGP and S/MIME are on an IETF standards track, it appears likely that S/MIME will emerge as the industry standard for commercial and organisational use, while PGP will remain the choice for personal e-mail security for many users. In this course we will only be looking at PGP. S/MIME is discussed in detail in the recommended text.

Cryptographic Keys and Key Rings

PGP makes use of four types of keys:

1. One-time session symmetric keys
2. Public keys
3. Private keys
4. Passphrase based symmetric keys

Two-Way Handshake Protocol

• Req: requests
• Accept: positive replies
• Refuse: negative replies ERROR ∈ Refuse: internal message indicating refusal
• Accept and Refuse are DISJOINT SETS
• At (. . .), both parties are sufficiently finished to go on with the next part of their tasks.

2.7 HTTP

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. HTTP has been in use by the World-Wide Web global information initiative since 1990. The first version of HTTP, referred to as HTTP/0.9, was a simple protocol for raw data transfer across the Internet. HTTP/1.0, as defined by RFC 1945 [6], improved the protocol by allowing messages to be in the format of MIME like messages, containing meta information about the data transferred and modifiers on the request/response semantics. However, HTTP/1.0 does not sufficiently take into consideration the effects of hierarchical proxies, caching, the need for persistent connections, or virtual hosts.

2.8 Digital Certificates

Digital Certificates provide a means of proving your identity in electronic transactions, much like a driver license or a passport does in face-to-face interactions. With a Digital Certificate, you can assure friends, business associates, and online services that the electronic information they receive from you are authentic. This document introduces Digital Certificates and answers questions you might have about how Digital Certificates.

Types of Digital Certificate

Identity Certificates

An Identity Certificate is one that contains a signature verification key combined with sufficient information to identify (hopefully uniquely) the keyholder. This type of certificate is much subtler than might first be imagined and will be considered in more detail later.

Accreditation Certificates

This is a certificate that identifies the key holder as a member of a specified group or organisation without necessarily identifying them. For example, such a certificate could indicate that the keyholder is a medical doctor or a lawyer. In many circumstances, a particular signature is needed to authorise a transaction but the identity of the key holder is not relevant. For example, pharmacists might need to ensure that medical prescriptions are signed by doctors but they do not need to know the specific identities of the doctors involved.

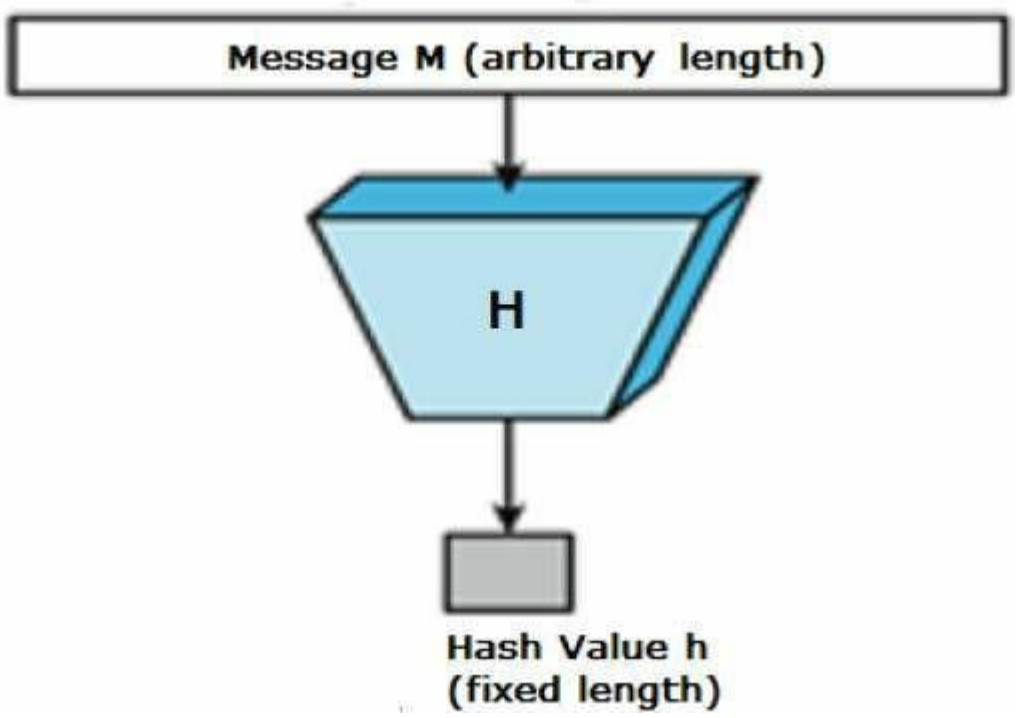
2.9 Hashing

Hashing means using some function or algorithm to map object data to some representative integer value.

Hash Functions

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called message digest or simply hash values. The following picture illustrated hash function −



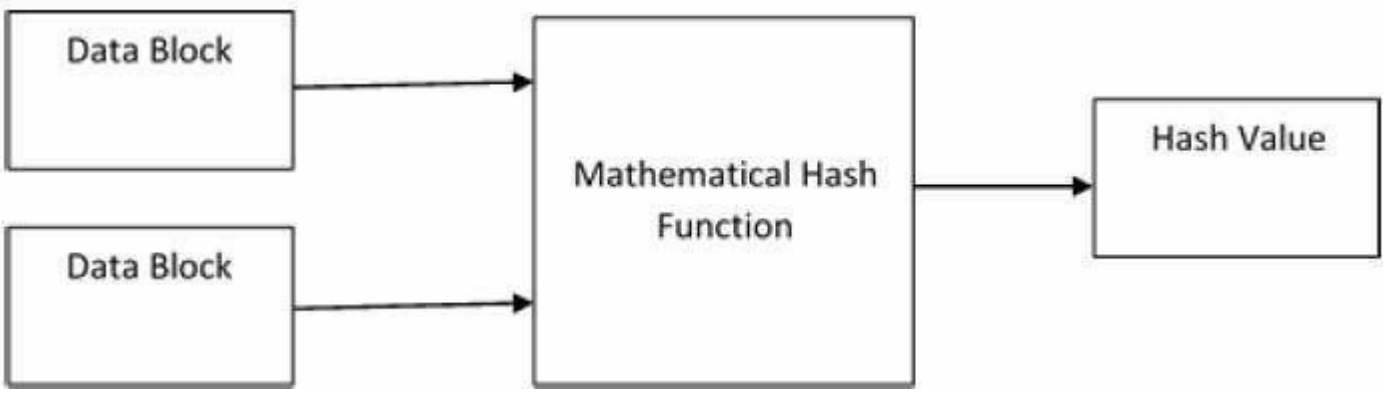
The typical features of hash functions are −

- *Fixed Length Output (Hash Value)*
  - *Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data.*
  - *In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions.*
  - *Since a hash is a smaller representation of a larger data, it is also referred to as a digest.*
  - *Hash function with n bit output is referred to as an n-bit hash function. Popular hash functions generate values between 160 and 512 bits.*

Design of Hashing Algorithms

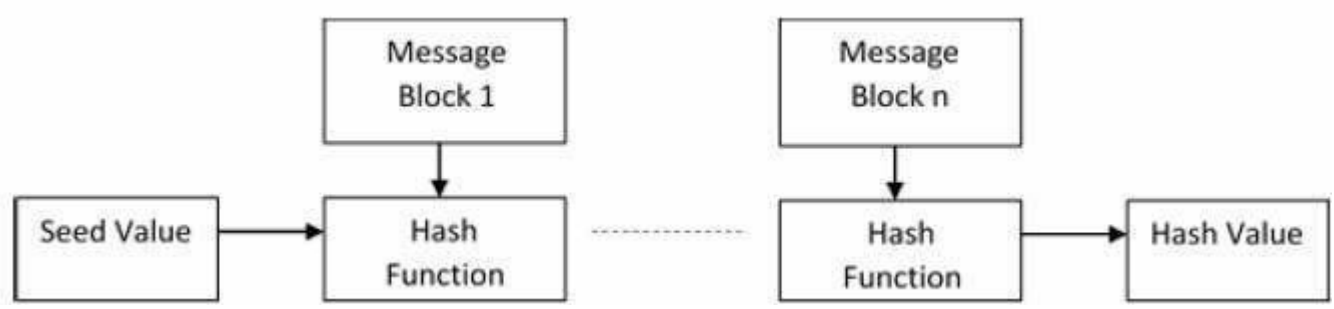
At the heart of a hashing is a mathematical function that operates on two fixed-size blocks of data to create a hash code. This hash function forms the part of the hashing algorithm.

The size of each data block varies depending on the algorithm. Typically the block sizes are from 128 bits to 512 bits. The following illustration demonstrates hash function −



Hashing algorithm involves rounds of above hash function like a block cipher. Each round takes an input of a fixed size, typically a combination of the most recent message block and the output of the last round.

This process is repeated for as many rounds as are required to hash the entire message. Schematic of hashing algorithm is depicted in the following illustration −



Hashing algorithm is a process for using the hash function, specifying how the message will be broken up and how the results from previous message blocks are chained together.

Popular Hash Functions

Let us briefly see some popular hash functions −

2.10 Message Digest (MD)

MD5 was most popular and widely used hash function for quite some years.

- *The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.*
- *MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file. For example, file servers often provide a pre-computed MD5 checksum for the files, so that a user can compare the checksum of the downloaded file to it.*
- *In 2004, collisions were found in MD5. An analytical attack was reported to be successful only in an hour by using computer cluster. This collision attack resulted in compromised MD5 and hence it is no longer recommended for use.*

2.11 Secure Hash Function (SHA)

Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, there are structurally different.

- *The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993. It had few weaknesses and did not become very popular. Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.*
- *SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.*

- *In 2005, a method was found for uncovering collisions for SHA-1 within practical time frame making long-term employability of SHA-1 doubtful.*
- *SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function.*
- *Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1. Hence, NIST called for new competitive hash function designs.*
- *In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. Keccak offers many benefits, such as efficient performance and*

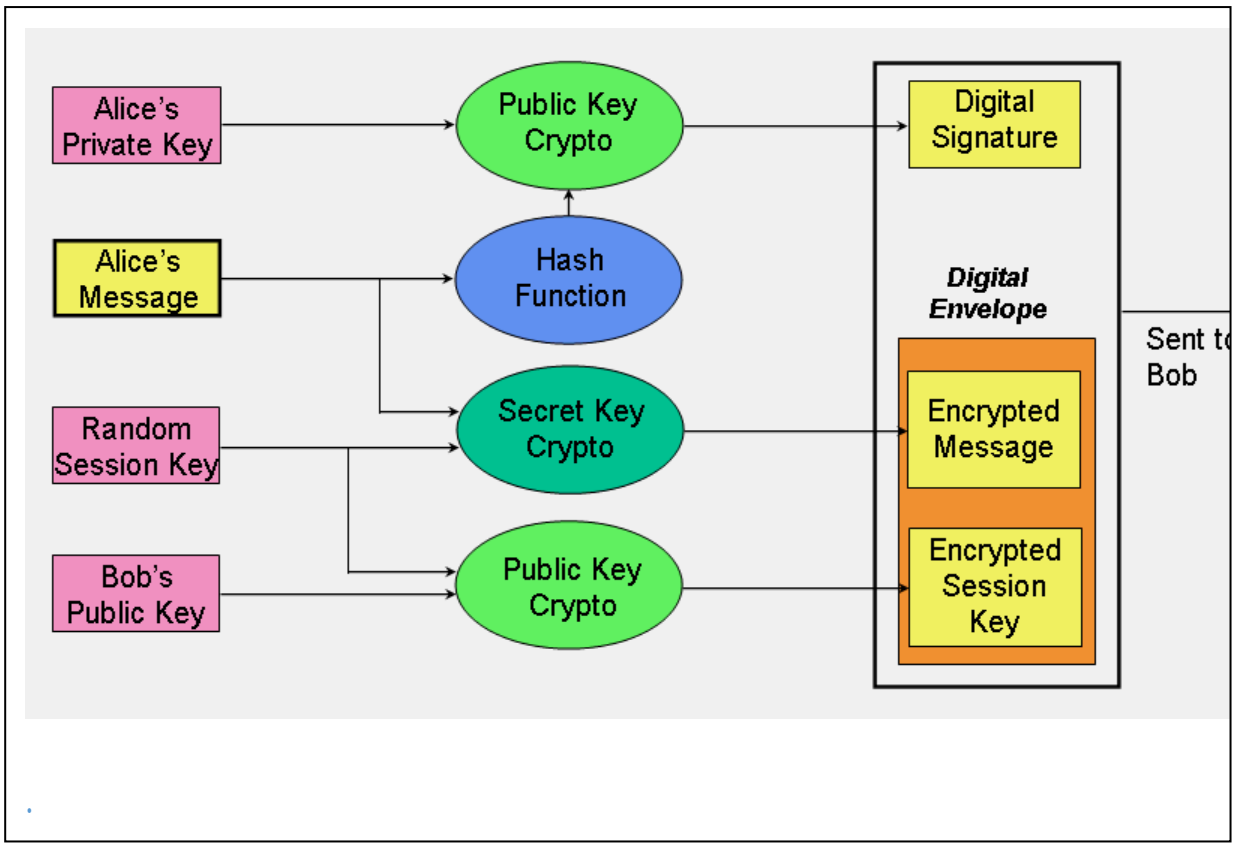
- *Applications of Hash Functions*

There are two direct applications of hash function based on its cryptographic properties.

Password Storage

Hash functions provide protection to password storage.

- *Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.*
- *The Password file consists of a table of pairs which are in the form (user id, h(P)).*
- *An intruder can only see the hashes of passwords, even if he accessed the password. He can neither logon using hash nor can he derive the password from hash value since hash function possesses the property of pre-image resistance.*



Above figure puts all of this together and shows how a hybrid cryptographic scheme combines all of these functions to form a secure transmission comprising a digital signature and digital envelope. In this example, the sender of the message is Alice and the receiver is Bob.

A digital envelope comprises an encrypted message and an encrypted session key. Alice uses secret key cryptography to encrypt her message using the session key, which she generates at random with each session. Alice then encrypts the session key using Bob's public key. The encrypted message and encrypted session key together form the digital envelope. Upon receipt, Bob recovers the session secret key using his private key and then decrypts the encrypted message.

The digital signature is formed in two steps. First, Alice computes the hash value of her message; next, she encrypts the hash value with her private key. Upon receipt of the digital signature, Bob recovers the hash value calculated by Alice by decrypting the digital signature with Alice's public key. Bob can then apply the hash function to Alice's original message, which he has already decrypted (see previous paragraph). If the resultant hash value is not the same as the value supplied by Alice, then Bob knows that the message has been altered; if the hash values are the same, Bob should believe that the message he received is identical to the one that Alice sent.

This scheme also provides non repudiation since it proves that Alice sent the message; if the hash value recovered by Bob using Alice's public key proves that

the message has not been altered, then only Alice could have created the digital signature. Bob also has proof that he is the intended receiver; if he can correctly decrypt the message.

2.12 Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

The steps followed in creating digital signature are :

1. *Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).*
2. *Digital signature is then transmitted with the message.(message + digital signature is transmitted)*
3. *Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).*
4. *The receiver now has the message digest.*
5. *The receiver can compute the message digest from the message (actual message is sent with the digital signature).*
6. *The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.*

Message digest is computed using one-way hash function, i.e. a hash fucntion in which computation of hash value of a is easy but computation of a from hash value of a is very difficult.

- *Public Key Certificates and Certificate Authorities*

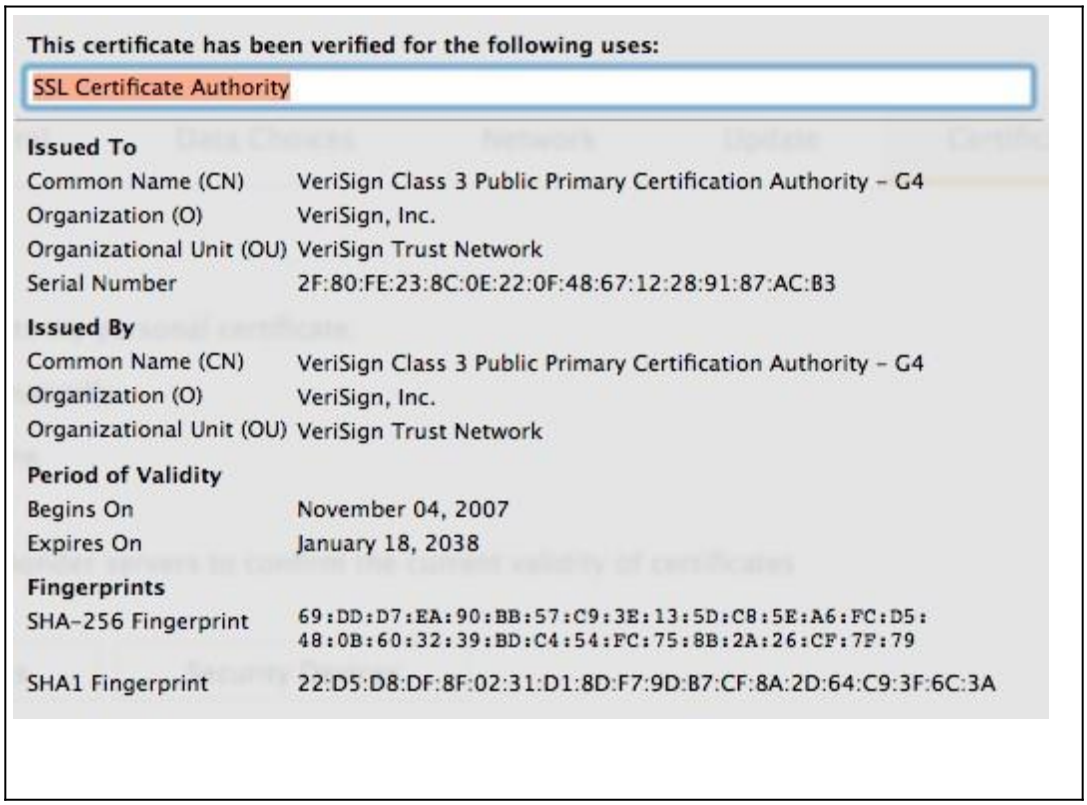
Certificates and Certificate Authorities (CA) are necessary for widespread use of cryptography for e-commerce applications. While a combination of secret and public key cryptography can solve the business issues discussed above, crypto cannot alone address the trust issues that must exist between a customer and vendor in the very fluid, very dynamic e-commerce relationship. How, for example, does one site obtain another party's public key? How does a recipient determine if a public key really belongs to the sender? How does the recipient know that the sender is using their public key for a legitimate purpose for which they are authorized? When does a public key expire? How can a key be revoked in case of compromise or loss?

For purposes of electronic transactions, certificates are digital documents. The specific functions of the certificate include:

- *Establish identity: Associate, or bind, a public key to an individual, organization, corporate position, or other entity.*
- *Assign authority: Establish what actions the holder may or may not take based upon this certificate.*

- *Secure confidential information (e.g., encrypting the session's symmetric key for data confidentiality).*

Typically, a certificate contains a public key, a name, an expiration date, the name of the authority that issued the certificate (and, therefore, is vouching for the identity of the user), a serial number, any pertinent policies describing how the certificate was issued and/or how the certificate may be used, the digital signature of the certificate issuer, and perhaps other information.



A sample abbreviated certificate is shown in above figure . This is a typical certificate found in a browser. The browser then checks the certificate's signature against the public key that it has stored; if there is a match, the certificate is taken as valid and the Web site verified by this certificate is considered to be "trusted."

The most widely accepted certificate format is the one defined in International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendation X.509. Rec. X.509 is a specification used around the world and any applications complying with X.509 can share certificates. Most certificates today comply with X.509 Version 3 and contain the information listed in Table below.

Contents of an X.509 V3 Certificate.

version number
certificate serial number
signature algorithm identifier

issuer's name and unique identifier *validity (or operational) period* *subject's name and unique identifier* *subject public key information* *standard extensions* *certificate appropriate use definition* *key usage limitation definition* *certificate policy information* *other extensions* *Application-specific* *CA-specific*

Certificate authorities are the repositories for public keys and can be any agency that issues certificates. A company, for example, may issue certificates to its employees, a college/university to its students, a store to its customers, an Internet service provider to its users, or a government to its constituents.

A digital certificate, an electronic document that contains the digital signature of the issuing certificate authority, binds together a public key with an identity and can be used to verify that a public key belongs to a particular person or entity.

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.
A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital signature is used to attach public key with a particular individual or an entity.

Digital certificate contains

1. *Name of certificate holder.*
2. *Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate*
3. *Expiration dates.*
4. *Copy of certificate holder's public key.(used for encrypting messages and digital signatures)*
5. *Digital Signature of the certificate issuing authority.*

Digital ceritifcate is also sent with the digital signature and the message.

- *IPSec*

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –

IPsec can be used to do the following things:

- *To encrypt application layer data.*
- *To provide security for routers sending routing data across the public internet.*
- *To provide authentication without encryption, like to authenticate that the data originates from a known sender*

Components of IP Security –

It has the following components:

1. *Encapsulating Security Payload (ESP) –*
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. *Authentication Header (AH) –*
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

2.13 Internet Key Exchange (IKE)

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Assocaition (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs)

Working of IP Security

1. *The host checks if the packet should be trasmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The in coming packets are also checked by the host that they are encrypted properly or not.*
2. *Then the IKE Phase 1 starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode which provides the greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly.*
3. *The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data accross the IP circuit.*
4. *Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.*
5. *Then the data is exchanged accross the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.*

6. *When the communacation between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts*

Unit 3

3.1 What Is a Computer Virus?

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.

It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action people will unknowingly continue the spread of a computer virus by sharing infecting files or sending emails with viruses as attachments in the email.

Fast Facts: *Attaches to an executable file, requires human action to spread.*

3.2 What Is a Worm?

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line.

Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In recent worm attacks such as the much-talked-about Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

Fast Facts: *Can replicate itself on system, does not require human action to spread.*

3.3 What Is a Trojan horse?

A Trojan Horse is full of as much trickery as the mythological Trojan Horse it was named after. The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.

When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdooron your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

3.4 Application level virus scanners

A virus scan is the process of using anti-virus software to scan and identify viruses in a computing device.

It is an information security process that aims to review and identify threatening viruses and programs. It is the core feature of anti-virus software.

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect from: malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms malicious LSPs, dialers, fraudtools adware and spyware Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT) and botnet DDoS attacks.

Unit 4

4.1 Firewall

In computing, a **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet

Firewalls are often categorized as either **network firewalls** or **host-based firewalls**. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

4.2 Hardware and Software Firewalls

Firewalls can be either hardware or software but the ideal configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins. Hardware firewalls can be purchased as a stand-alone product but are typically found in broadband routers, and should be considered an important part of your system security and network set-up. Most hardware firewalls will have a minimum

of four network ports to connect other computers, but for larger networks, a business networking firewall solution is available.

4.3 Firewall Filtering Techniques

Firewalls are used to protect both home and corporate networks. A typical firewall program or hardware device filters all information coming through the Internet to your network or computer system.

There are several types of firewall techniques that will prevent potentially harmful information from getting through:

- **Packet Filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- **Application Gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- **Circuit-level Gateway:** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- **Proxy Server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

4.4 Next Generation Firewall (NGFW)

Firewalls called *next generation firewalls (*NGFW), work by filtering network and Internet traffic based upon the applications or traffic types using specific ports. Next Generation Firewalls (NGFWs) blend the features of a standard firewall with quality of service (QoS) functionalities in order to provide smarter and deeper inspection

Firewall Limitations

A firewall is a crucial component of securing your network and is designed to address the issues of data integrity or traffic authentication (via stateful packet inspection) and confidentiality of your internal network (via NAT). Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. The importance of including a firewall in your security strategy is apparent; however, firewalls do have the following limitations:

- A firewall cannot prevent users or attackers with modems from dialing in to or out of the internal network, thus bypassing the firewall and its protection completely.
- Firewalls cannot enforce your password policy or prevent misuse of passwords. Your password policy is crucial in this area because it outlines acceptable conduct and sets the ramifications of noncompliance.
- Firewalls are ineffective against nontechnical security risks such as social engineering, as discussed in Chapter 1, “There Be Hackers Here.”
- Firewalls cannot stop internal users from accessing websites with malicious code, making user education critical.
- Firewalls cannot protect you from poor decisions.
- Firewalls cannot protect you when your security policy is too lax.

Unit 5

5.1 Intrusion detection system

An **intrusion detection system** (**IDS**) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filteringtechniques to distinguish malicious activity from false alarms.[1]

IDS types range in scope from single computers to large networks.[2] The most common classifications are **network intrusion detection systems** (**NIDS**) and **host-based intrusion detection systems** (**HIDS**). A system that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of an NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware); and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Some IDS products have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an **intrusion prevention system**.[3] Intrusion detection systems can also serve specific purposes by augmenting them with custom tools, such as using a honeypot to attract and characterize malicious traffic.[4]

5.2 Limitations of Intrusion detection system

- Noise can severely limit an intrusion detection system's effectiveness. Bad packets generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate.[28]

- It is not uncommon for the number of real attacks to be far below the number of false-alarms. Number of real attacks is often so far below the number of false-alarms that the real attacks are often missed and ignored.[28][*needs update*]
- Many attacks are geared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to newer strategies.[28]
- For signature-based IDS, there will be lag between a new threat discovery and its signature being applied to the IDS. During this lag time, the IDS will be unable to identify the threat.[27]
- It cannot compensate for weak identification and authentication mechanisms or for weaknesses in network protocols. When an attacker gains access due to weak authentication mechanisms then IDS cannot prevent the adversary from any malpractice.
- Encrypted packets are not processed by most intrusion detection devices. Therefore, the encrypted packet can allow an intrusion to the network that is undiscovered until more significant network intrusions have occurred.
- Intrusion detection software provides information based on the network address that is associated with the IP packet that is sent into the network. This is beneficial if the network address contained in the IP packet is accurate. However, the address that is contained in the IP packet could be faked or scrambled.
- Due to the nature of NIDS systems, and the need for them to analyse protocols as they are captured, NIDS systems can be susceptible to the same protocol-based attacks to which network hosts may be vulnerable. Invalid data and TCP/IP stack attacks may cause an NIDS to crash

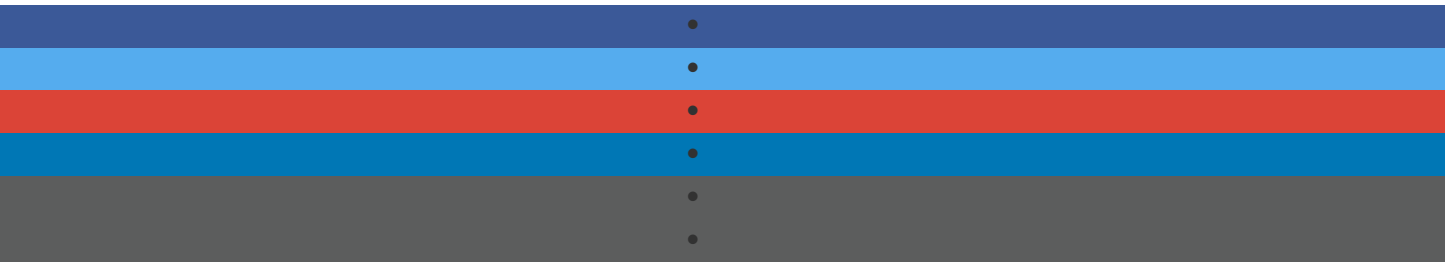
5.3 Teardrop Attack

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

One of the fields in an IP header is the “fragment offset” field, indicating the starting position, or offset, of the data contained in a

fragmented packet relative to the data in the original packet. If the sum of the offset and size of one fragmented packet differs from that of the next fragmented packet, the packets overlap. When this happens, a server vulnerable to teardrop attacks is unable to reassemble the packets - resulting in a denial-of-service condition.

5.4 countermeasure



A countermeasure is an action, process, device, or system that can prevent, or mitigate the effects of, threats to a computer, server or network. In this context, a threat is a potential or actual adverse event that may be malicious or incidental, and that can compromise the assets of an enterprise or the integrity of a computer or network.

Countermeasures can take the form of software, hardware and modes of behavior. Software countermeasures include:

- personal firewalls
- application firewalls
- anti-virus software
- pop-up blockers
- spyware detection/removal programs.

The most common hardware countermeasure is a router that can prevent

the IP address of an individual computer from being directly visible on the Internet. Other hardware countermeasures include:

- biometric authentication systems
- physical restriction of access to computers and peripherals
- intrusion detectors
- alarms.

Unit 6

6.1 Cyber Assests

Your first port of call in a cyber crisis

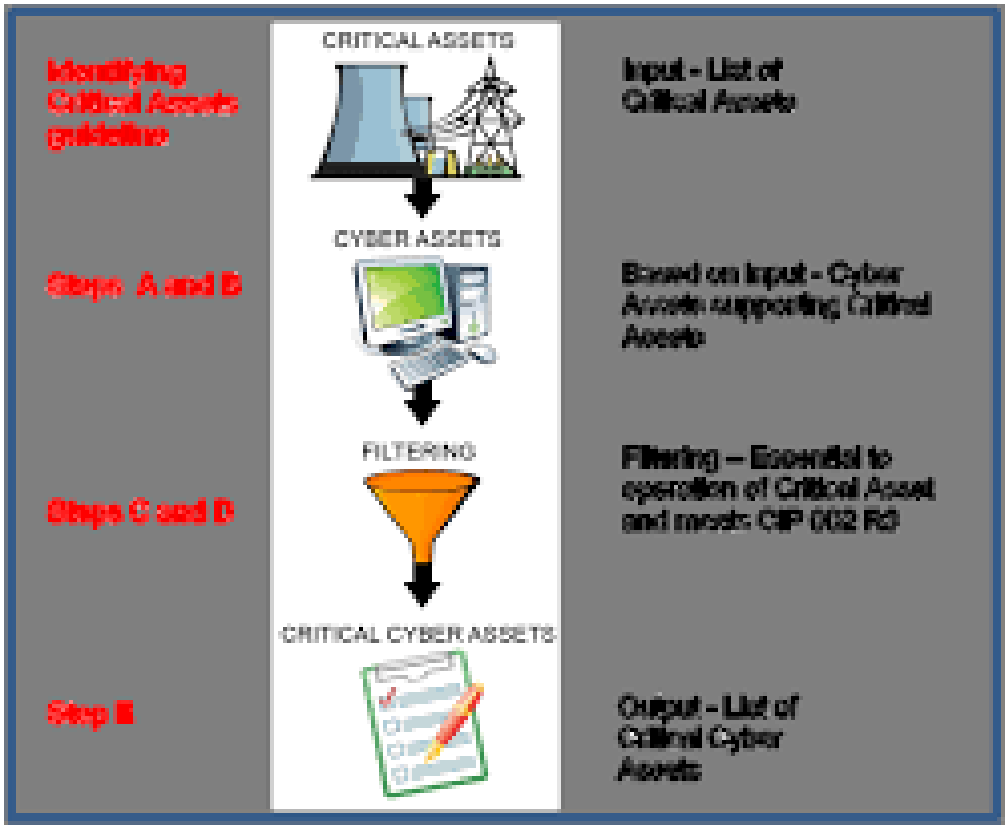
Fines for breaching obligations in relation to a cyber attack can be up to 4% of global turnover. Clifford Chance Cyber Assist should be your first port of call in a cyber crisis.

In the event of a cyber attack, Clifford Chance Cyber Assist helps you to manage the risk. We outline the steps which regulators around the world expect you to take in the vital hours and days which follow. Our team is immediately available at the push of a button. Global cyber specialists from Clifford Chance can be contacted directly through the app for urgent assistance – day or night.

Key contacts and information can be accessed through the app when your other technology is compromised – it's held locally on your smartphone device, not on a central IT platform. To make sure you have complete access, we recommend downloading the app on your personal device.

The app also provides access to a wide range of Clifford Chance cyber-related information, including summaries from our new global legal and regulatory report: "Cyber Security – what regulators are saying around the globe".
This app has been designed for Clifford Chance clients. To gain full access to the app, please email the Cyber Assist team or speak to your Clifford Chance relationship team.

6.2 Configuration policy as per standards



6.3 Disposal Policy

Assets Disposal Policy

The **Asset Disposal** Form is to be completed each time an **asset** covered by this**policy** is to be **disposed** of. At the end of the **disposal** process, the Form needs to be provided to Finance.

Unit 7

7.1 VPN

A virtual private network, or VPN, extends across a public or shared network, and acts like a tunnel so you can exchange data securely and anonymously across the internet as if you were connected directly to a private network. Watch What is a VPN? video below, to learn more about Hotspot Shield VPN.

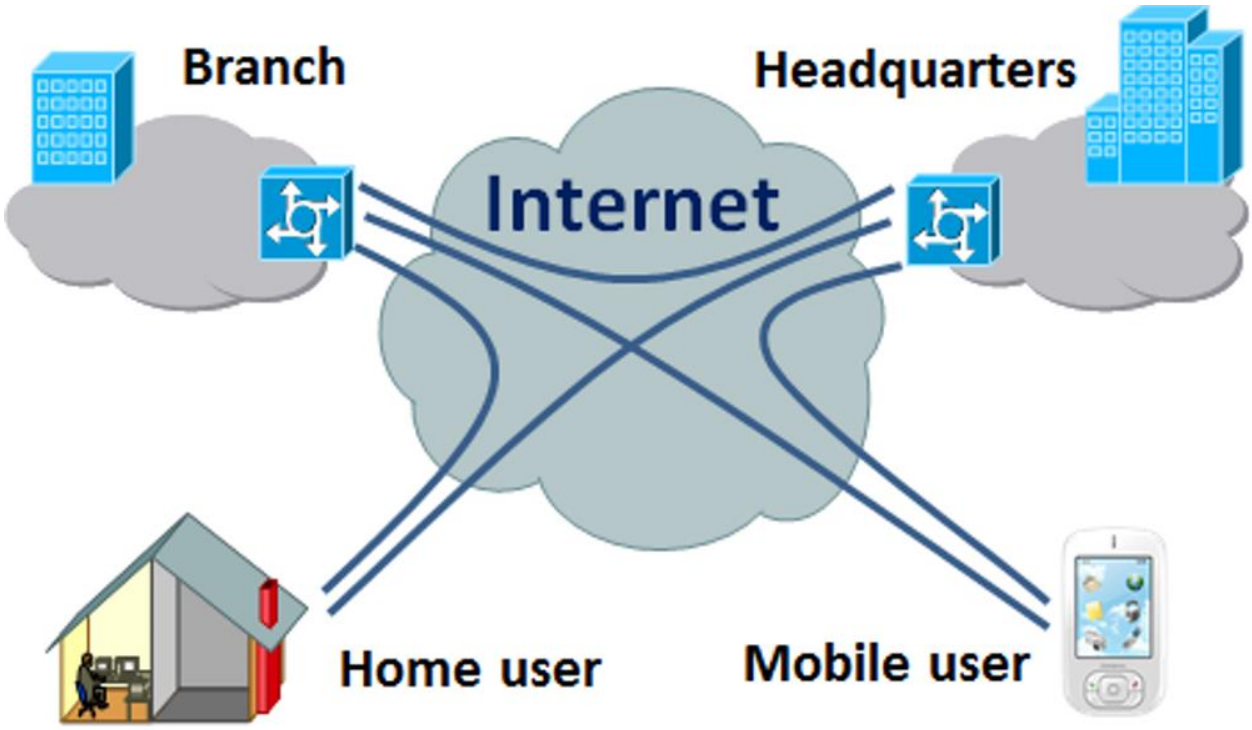
VPN explained

Information traveling between a connected device (computer, smartphone, tablet) and a VPN server is encrypted, and as a result, any applications running on the VPN network benefit from the security, functionality, and strength of the private network.

What many people don't know is your home Wi-Fi network can be just as unsafe as a Public Wi-Fi network. Additional layers of security are needed to keep hackers, cyber criminals, and data thieves at bay. A VPN provides the privacy and data security you need.

A top-tier VPN service, like Hotspot Shield VPN, has the following advantages:

- Helps you avoid censorship blocks
- Masks your IP address
- Hides your physical location
- Encrypts data between your computer and the VPN server
- Does not log your browsing activity
- Allows you to access popular streaming services like Netflix and YouTube from other countries



7.2 VPN Diagram

Client VPN OS Configuration

Table of contents

This article outlines instructions to configure a client VPN connection on commonly-used operating systems. For more information about client VPN, please refer to our documentation.

This article outlines instructions to configure a client VPN connection on commonly-used operating systems. For more information about client VPN, please refer to our documentation.

Android

To configure an Android device to connect to the Client VPN, follow these steps:

- Navigate to **Settings** -> **Wireless & Networks** -> **VPN**

- **Click the Plus Icon** to add an additional VPN profile

- Enter a **VPN Name** for the connection.
- For the **Type** drop-down select **L2TP/IPSEC PSK VPN**
- Enter the public IP (found in Dashboard, under **Security appliance > Monitor > Appliance status > Uplink**) of the MX device under **Server address**.
- Enter the pre-shared key under **IPSec pre-shared key**.

- Save the configuration.

  You will be prompted for credentials when you connect.

7.3 Internet Key Exchange (IKE) for VPN

he IKE process allows the VPN peers at both ends of the tunnel to encrypt and decrypt packets using mutually agreed-upon keys or certificate and method of encryption. The IKE process occurs in two phases: IKE Phase 1 and IKE Phase 2. Each of these phases use keys and encryption algorithms that are defined using cryptographic profiles— IKE crypto profile and IPSec crypto profile—and the result of the IKE negotiation is a Security Association (SA). An SA is a set of mutually agreed-upon keys and algorithms that are used by both VPN peers to allow the flow of data across the VPN tunnel. The following illustration depicts the key exchange process for setting up the VPN tunnel:

Unit 8

8.1 Disaster recovery (DR)

Disaster recovery (DR) is an area of security planning that aims to protect an organization from the effects of significant negative events. DR allows an organization to maintain or quickly resume mission-critical functions following a disaster.

A disaster can be anything that puts an organization's operations at risk, from a cyberattack to equipment failures to natural disasters. The goal with DR is for a business to continue operating as close to normal as possible. The disaster recovery process includes planning and testing, and may involve a separate physical sitz`e for restoring operations.

The importance of disaster recovery: RPO and RTO

As businesses have become more reliant on high availability, the tolerance for downtime has decreased.

A disaster can have a devastating effect on a business. Studies have shown that many businesses fail after experiencing a significant data loss, but DR can help.

Recovery point objective (RPO) and recovery time objective (RTO) are two important measurements in disaster recovery and downtime.

RPO is the maximum age of files that an organization must recover from backup storage for normal operations to resume after a disaster. The recovery point objective determines the minimum frequency of backups. For example, if an

organization has an RPO of four hours, the system must back up at least every four hours.

Disaster recovery involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions,[1] as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery can therefore be considered as a subset of business continuity.

8.2 Disaster recovery for virtual servers

> ***Server virtualisation helps make disaster recovery easier by representing everything in logical terms and doing away with the need for a physical replica of your environment.***

The rise of virtualized x86 servers is changing the disaster recovery (DR) process, making it easier and more cost effective while requiring more careful planning .

A traditional disaster recovery setup – with a second entirely physical environment – is expensive and often requires companies to prioritise the machines they most need to safeguard, leaving others exposed. Server virtualisation helps make disaster recovery easier by representing

everything in logical terms and doing away with the need for a physical replica of your environment.

A medium-sized organisation with 100 servers, for example, could expect to pay as much as £150,000 per annum for DR services and only cover a small percentage of its servers, estimated Andrew Cooke, a principal consultant at City of London-based services provider Intercept IT. But with virtualisation they can cover everything for the same cost.

"In traditional DR arrangements, companies often only protect about 20% of their servers – they'll pick and choose due to the cost involved. But in a virtualised environment, we say 'why not cover everything because it won't cost you any more?'" Cooke said.

So while using virtual servers improves the DR process, it also changes it and makes planning more crucial.

8.3 Cluster

clustering *is the task of grouping a set of objects in such a way that objects in the same group (called a* ***cluster****) are more similar (in some sense) to each other than to those in other groups (clusters). It is a main task of exploratory data mining, and a common technique for statistical data analysis, used in many fields, including machine learning, pattern recognition, image analysis, information retrieval, bioinformatics, data compression, and computer graphics.*

Cluster analysis itself is not one specific algorithm, but the general task to be solved. It can be achieved by various algorithms that differ significantly in their understanding of what

constitutes a cluster and how to efficiently find them. Popular notions of clusters include groups with small distances between cluster members, dense areas of the data space, intervals or particular statistical distributions. Clustering can therefore be formulated as a multi-objective optimization problem. The appropriate clustering algorithm and parameter settings (including parameters such as the distance function to use, a density threshold or the number of expected clusters) depend on the individual data set and intended use of the results. Cluster analysis as such is not an automatic task, but an iterative process of knowledge discovery or interactive multi-objective optimization that involves trial and failure. It is often necessary to modify data preprocessing and model parameters until the result achieves the desired properties.

8.4 RAIR

RAID, or “Redundant Arrays of Independent Disks” is a technique which makes use of a combination of multiple disks instead of using a single disk for increased performance, data redundancy or both. The term was coined by David Patterson, Garth A. Gibson, and Randy Katz at the University of California, Berkeley in 1987.

RAID (**Redundant Array of Independent Disks**, originally **Redundant Array of Inexpensive Disks**) is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both. This was in contrast to the previous concept of highly reliable mainframe disk drives referred to as "single large expensive disk" (SLED).[1] [2]

Data is distributed across the drives in one of several ways, referred to as RAID levels, depending on the required level of redundancy and performance. The different schemes, or data distribution layouts, are named by the word "RAID" followed by a number, for example RAID 0 or RAID 1. Each scheme, or RAID level, provides a different balance among the key goals: reliability, availability, performance, and capacity. RAID levels greater than RAID 0 provide protection against unrecoverable sector read errors, as well as against failures of whole physical drives.

Why data redundancy?

Data redundancy, although taking up extra space, adds to disk reliability. This means, in case of disk failure, if the same data is also backed up onto another disk, we can retrieve the data and go on with the operation. On the other hand, if the data is spread across just multiple disks without the RAID technique, the loss of a single disk can affect the entire data.